WHAT IS CLAIMED IS:

1. A data processing apparatus, comprising:
   - a memory store;
   - a data bus connected to the memory store, the data bus being adapted for transporting data to and from the memory store;
   - a processing entity operative to release read and write commands towards the memory store, the write command being accompanied by first data intended to be written to the memory store;
   - an encryption module communicatively coupled to the processing entity and to the data bus;
   - upon the processing entity releasing a write command accompanied by said first data, the encryption module being operative to encrypt, in accordance with an encryption key, said first data and send an encrypted version of said first data onto the data bus for writing into the memory store;
   - upon the processing entity releasing a read command, the encryption module being operative to decrypt, in accordance with a decryption key, an encrypted version of second data received from the memory store via the data bus and provide said second data to the processing entity.

2. The data processing apparatus defined in claim **1**, the processing entity and the encryption module being implemented by a common application-specific integrated circuit.

3. The data processing apparatus defined in claim **2**, wherein the encryption module is adapted to store the encryption key and the decryption key in a portion of a volatile memory.

4. The data processing apparatus defined in claim **3**, wherein the encryption module is adapted to erase the portion of the volatile memory in response to a signal received from a control module.

5. The data processing apparatus defined in claim **4**, further comprising:
   - a control module operative to provide the encryption key and the decryption key to the encryption module.

6. The data processing apparatus defined in claim **5**, wherein the control module is operative to change the encryption key in response to instructions received from a host entity.

7. The data processing apparatus defined in claim **6**, wherein the control module is operative to change the encryption key in accordance with a policy applied in response to stimuli received from a host entity and a user of the data processing apparatus.

8. The data processing apparatus defined in claim **1**, wherein the memory store comprises volatile memory.

9. The data processing apparatus defined in claim **1**, wherein the memory store comprises non-volatile memory.

10. The data processing apparatus defined in claim **1**, wherein the encryption key and the decryption key are identical.

11. The data processing apparatus defined in claim **1**, further comprising a selection module connected between the processing entity and the encryption module, the selection module also being connected to the memory store, the selection module being capable of selectively operating in a selected one of a first operational state in which said first and second data is exchanged directly with the memory store and a second operational state in which said first and second data is exchanged with the encryption module.

12. The data processing apparatus defined in claim **11**, wherein the processing entity is operative to provide a control signal to the selection module, the control signal being indicative of the selected operational state of the selection module.

13. The data processing apparatus defined in claim **11**, wherein the processing entity is operative to provide messages to the selection module, the messages being indicative of the selected operational state of the selection module for selected data to be exchanged with the memory store.

14. The data processing apparatus defined in claim **13**, wherein the messages accompany the data to be exchanged with the memory store.

15. An end user device for communication with a server, comprising:
    - a control entity operative to support a session with the server for an authenticated user;
    - a memory store operative to store sensitive information during the session;
    - the control entity further operative to (i) determine whether confidentiality of the sensitive information stored in the memory store is to be preserved and (ii) responsive to determining that confidentiality of the sensitive information stored in the memory store is to be preserved, taking an action to preserve confidentiality of the sensitive information stored in the memory store.

16. The end user device defined in claim **15**, further comprising a user interface for interfacing with the authenticated user and a network interface for interfacing with the server.

17. The end user device defined in claim **16**, wherein the control entity being operative to determine whether confidentiality of the sensitive information stored in the memory store is to be preserved comprises the control entity being operative to apply a policy based on stimuli received via the user interface and the network interface.

18. The end user device defined in claim **17**, wherein said stimuli comprise user commands received via the user interface and wherein determining that confidentiality of the sensitive information stored in the memory store is to be preserved comprises detecting a user command to terminate the session.

19. The end user device defined in claim **18**, wherein said stimuli comprise user commands received via the user interface and wherein determining that confidentiality of the sensitive information stored in the memory store is to be preserved comprises detecting a user command to suspend the session.

20. The end user device defined in claim **19**, wherein said stimuli comprise user commands received via the user interface and wherein determining that confidentiality of the

sensitive information stored in the memory store is to be preserved comprises detecting a user command to authenticate a new user other than the authenticated user.

21. The end user device defined in claim **20**, wherein said stimuli comprise network commands received via the network interface and wherein determining that confidentiality of the sensitive information stored in the memory store is to be preserved comprises detecting a network command to terminate the session.

22. The end user device defined in claim **21**, wherein said stimuli comprise network commands received via the network interface and wherein determining that confidentiality of the sensitive information stored in the memory store is to be preserved comprises detecting a network command to suspend the session.

23. The end user device defined in claim **22**, wherein said stimuli comprise pilot messages received via the network interface and wherein determining that confidentiality of the sensitive information stored in the memory store is to be preserved comprises detecting a prolonged absence of pilot messages received from the network interface.

24. The end user device defined in claim **23**, further comprising an RF-ID detector operative to detecting an identification code of a potential user proximate the end user device, the RF-ID detector further operative to provide a detected identification code to the control entity.

25. The end user device defined in claim **24**, the control entity being adapted to effect a comparison of the detected identification code to an identification code associated with the authenticated user.

26. The end user device defined in claim **25**, the control entity being adapted to estimate a distance between the authenticated user and the end user device based on the comparison.

27. The end user device defined in claim **26**, wherein said stimuli comprise the distance estimated by the control entity and wherein determining that confidentiality of the sensitive information stored in the memory store is to be preserved comprises detecting that said distance exceeds a predetermined threshold.

28. The end user device defined in claim **26**, wherein said stimuli comprise the distance estimated by the control entity and wherein determining that confidentiality of the sensitive information stored in the memory store is to be preserved comprises detecting that said distance continuously exceeds a predetermined threshold for a predetermined amount of time.

29. The end user device defined in claim **26**, wherein said stimuli comprise the distance estimated by the control entity and wherein determining that confidentiality of the sensitive information stored in the memory store is to be preserved comprises detecting that an integral of said distance over time exceeds a predetermined threshold.

30. The end user device defined in claim **29**, the control entity being adapted to receive an indication of a distance between the authenticated user and the end user device.

31. The end user device defined in claim **30**, wherein said stimuli comprise said distance and wherein determining that confidentiality of the sensitive information stored in the memory store is to be preserved comprises detecting that said distance exceeds a predetermined threshold.

32. The end user device defined in claim **30**, wherein said stimuli comprise the distance and wherein determining that confidentiality of the sensitive information stored in the memory store is to be preserved comprises detecting that said distance continuously exceeds a predetermined threshold for a predetermined amount of time.

33. The end user device defined in claim **30**, wherein said stimuli comprise the distance and wherein determining that confidentiality of the sensitive information stored in the memory store is to be preserved comprises detecting that an integral of said distance over time exceeds a predetermined threshold.

34. The end user device defined in claim **15**, wherein the control entity being operative to take an action to preserve confidentiality of the sensitive information stored in the memory store comprises rendering the sensitive information stored in the memory store inaccessible to potential users of the end user device other than the authenticated user.

35. The end user device defined in claim **15**, wherein the control entity being operative to take an action to preserve confidentiality of the sensitive information stored in the memory store comprises erasing the sensitive information from the memory store.

36. The end user device defined in claim **15**, wherein the control entity being operative to take an action to preserve confidentiality of the sensitive information stored in the memory store comprises scrambling the sensitive information in the memory store.

37. The end user device defined in claim **16**, wherein the control entity being operative to take an action to preserve confidentiality of the sensitive information stored in the memory store comprises disabling the user interface.

38. The end user device defined in claim **15**, further comprising
    - a data bus connected to the memory store, the data bus being adapted for transporting data to and from the memory store;
    - an encryption module communicatively coupled to the control entity and to the data bus;
    - the control entity being further operative to release read and write commands towards the memory store, the write command being accompanied by first data intended to be written to the memory store;
    - upon the control entity releasing a write command accompanied by said first data, the encryption module being operative to encrypt, in accordance with an encryption key, said first data and send an encrypted version of said first data onto the data bus for writing into the memory store;
    - upon the control entity releasing a read command, the encryption module being operative to decrypt, in accordance with a decryption key, an encrypted version of second data received from the memory store via the data bus and provide said second data to the control entity.

39. The end user device defined in claim **38**, wherein the control entity being operative to take an action to preserve confidentiality of the sensitive information stored in the memory store comprises changing the decryption key.

40. The end user device defined in claim **38**, wherein the control entity being operative to take an action to preserve confidentiality of the sensitive information stored in the memory store comprises deleting the decryption key.

41. The end user device defined in claim **38**, wherein the control entity being operative to take an action to preserve confidentiality of the sensitive information stored in the memory store comprises causing the encryption module to use a new decryption key different from the previous decryption key.

42. The end user device defined in claim **41**, wherein the control entity being operative to take an action to preserve confidentiality of the sensitive information stored in the memory store further comprises storing the previous decryption key prior to causing the encryption module to use the new decryption key.

43. The end user device defined in claim **42**, the control entity further operative to (iii) determine whether confidentiality of the sensitive information stored in the memory store no longer needs to be preserved and (iv) responsive to determining that confidentiality of the sensitive information stored in the memory store no longer needs to be preserved, cause the encryption module to use said previous decryption key.

44. The end user device defined in claim **15**, the control entity further operative to (iii) determine whether confidentiality of the sensitive information stored in the memory store no longer needs to be preserved and (iv) responsive to determining that confidentiality of the sensitive information stored in the memory store no longer needs to be preserved, take an action to reverse the action previously taken to preserve confidentiality of the sensitive information stored in the memory store.

45. The end user device defined in claim **44**, wherein the control entity being operative to determine whether confidentiality of the sensitive information stored in the memory store no longer needs to be preserved comprises the control entity being operative to apply a policy based on stimuli received via the user interface and the network interface.

46. The end user device defined in claim **45**, wherein said stimuli comprise user commands received via the user interface and wherein determining that confidentiality of the

sensitive information stored in the memory store no longer needs to be preserved comprises detecting a host command to unsuspend a suspended session.

47. The end user device defined in claim **15** being a mobile wireless device.

48. The end user defined in claim **15**, further comprising a label indicative of an inability to function outside a predetermined location.

49. A method comprising
- supporting a session with the server for an authenticated user;
- storing sensitive information during the session;
- determining whether confidentiality of the sensitive information stored in the memory store is to be preserved;
- responsive to determining that confidentiality of the sensitive information stored in the memory store is to be preserved, taking an action to preserve confidentiality of the sensitive information stored in the memory store.

50. The method defined in claim **49**, wherein the sensitive information comprises healthcare information

51. A method, comprising:
- establishing a healthcare session with an end user device servicing an authenticated user;
- providing sensitive healthcare information to the end user device for storage thereon during the healthcare session;
- detecting existence of a requirement to preserve confidentiality of the sensitive healthcare information;
- responsive to the detecting, sending a message to the end user device instrumental in causing the end user device to preserve the confidentiality of the sensitive healthcare information.

52. The method defined in claim **51**, the healthcare session being established between the end user device and an application server, wherein detecting existence of a requirement to

preserve confidentiality of the sensitive healthcare information comprises detecting termination of the session at the application server.

53. The method defined in claim **51**, wherein detecting existence of a requirement to preserve confidentiality of the sensitive healthcare information comprises detecting a distance between the authenticated user and the end user device and determining that the distance exceeds a predetermined threshold.

54. The method defined in claim **51**, wherein detecting existence of a requirement to preserve confidentiality of the sensitive healthcare information comprises detecting a distance between the authenticated user and the end user device and determining that the distance continuously exceeds a predetermined threshold for a predetermined period of time.

55. The method defined in claim **51**, wherein detecting existence of a requirement to preserve confidentiality of the sensitive healthcare information comprises detecting a distance between the authenticated user and the end user device and determining that an integral of the distance over time exceeds a predetermined threshold.

56. A network attachment process for an end user device, comprising:
- receiving operational characteristics of the end user device;
- selecting operating code for use by the end user device on the basis of the operational characteristics of the end user device;
- downloading the selected operating system code onto the end user device.

57. A host entity for use in a network, comprising:
- a terminal identification module adapted to receive operational characteristics of an end user device;
- an operating system server adapted to select operating code for use by the end user device on the basis of the operational characteristics of the end user device;
- the operating system server further adapted to transmit the selected operating system code to the end user device.

58. A network attachment process for an end user device, comprising:

- transmitting first operating system code to the end user device to enable the end user device to transmit a message requesting authentication of a user;
- responsive to successful authentication of the user, transmitting second operating system code to enable continued use of the end user device by the user.

59. The process defined in claim **58**, further comprising:
- receiving operational characteristics of the end user device;
- wherein the first operating code transmitted to the end user device is selected on the basis of the operational characteristics of the end user device.

60. The process defined in claim **58**, further comprising:
- receiving customization preferences from the end user device;
- wherein the second operating code transmitted to the end user device is selected on the basis of the received customization preferences.